

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-306760

(43)Date of publication of application : 29.10.1992

(51)Int.Cl. G06F 15/00

G06F 15/30

G06F 15/30

G06K 17/00

G07F 7/12

G09C 1/00

(21)Application number : 03-098017

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

(22)Date of filing : 03.04.1991

(72)Inventor : MORITA HIKARI
KURIHARA SADAMI

(54) RECOGNITION METHOD FOR POSSESSOR OF CARDS

(57)Abstract:

PURPOSE: To securely recognize the right possessor of cards without increasing the burden on a user in an information processing service system using the cards.

CONSTITUTION: A processing/storage means is embedded in the belongings 1 (watch, ring and the like) of the possessor of the cards 2. The belongings 1 and the cards 2 previously share the same initial values of ciphered key data and output feedback data. At the time of using the cards 2, the belongings 1 cipher and update the output feedback data with ciphered key data and transmit the updated data to the cards 2. The cards 2 cipher and update the output feedback data with ciphered key data and compare the updated data with the updated data from the cards 1. When they coincide, the cards concerned are set to a usable state. Here, the access of an information processor 3 by the cards 2 becomes possible.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平4-306760

(43) 公開日 平成4年(1992)10月29日

(51) Int. Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 15/00	9 3 0 B	7323-5L		
	F	7328-5L		
15/30	3 4 0	6798-5L		
	3 5 0	6798-5L		
		8818-3E		
		G 0 7 F 7/08		B

審査請求 未請求 請求項の数 6 (全 10 頁) 最終頁に続く

(21) 出願番号 特願平3-98017

(22) 出願日 平成3年(1991)4月3日

(71) 出願人 000004228

日本電信電話株式会社

東京都千代田区内幸町一丁目1番6号

(72) 発明者 森田 光

東京都千代田区内幸町一丁目1番6号 日

本電信電話株式会社内

(72) 発明者 栗原 定見

東京都千代田区内幸町一丁目1番6号 日

本電信電話株式会社内

(74) 代理人 弁理士 鈴木 誠

(54) 【発明の名称】 カード類の所有者確認方法

(57) 【要約】

【目的】 カード類を利用する情報処理サービスシステムにおいて、使用者の負担を増加させることなく、確実にカード類の正当所有者の確認を行う。

【構成】 カード類2の所有者の携帯物1 (時計、指輪等) に処理/記憶手段を埋め込み、携帯物1とカード類2とに、予め同一の暗号鍵データと出力帰還データの初期値を共有させる。カード類2を利用する際、携帯物1は、その出力帰還データを暗号鍵データで暗号化して更新すると共に、該更新データをカード類2に送る。カード類2でも、その出力帰還データを暗号鍵データで暗号化して更新し、該更新データとカード類1からの更新データを比較し、一致したら当該カード類を利用可状態とする。ここで初めて、カード類2による情報処理装置3のアクセスが可能となる。



1

【特許請求の範囲】

【請求項1】 利用可と利用不可の状態をとり、利用可の場合に情報処理装置に対して処理を依頼でき、処理終了で利用不可となるカード類の所有者を確認する方法であって、前記カード類の所有者が携帯する携帯物に、あらかじめ定められた暗号鍵データを格納する手段と、あらかじめ定められた初期値をとり、その後更新される出力帰還データを格納する手段と、前記暗号鍵データにより前記出力帰還データを暗号化して更新する手段と、前記更新された出力帰還データを前記カード類に送信する手段を設け、前記カード類には、前記携帯物が送信した出力帰還データを受信する手段と、あらかじめ定められた暗号鍵データを格納する手段と、あらかじめ定められた初期値をとり、その後更新される出力帰還データを格納する手段と、前記暗号鍵データにより前記出力帰還データを暗号化して更新する手段と、前記更新された出力帰還データと前記携帯物から受信した出力帰還データとを比較して、当該カード類の利用可または利用不可を決定する手段とを設け、前記携帯物とカード類の暗号鍵データ、出力帰還データの初期値を一致させ、所有者の処理要求の度に、前記携帯物の出力帰還データと前記カード類の出力帰還データを更新せしめて同期をとることを特徴とするカード類の所有者確認方法。

【請求項2】 前記携帯物とカード類が同時に発行されない場合のために、前記カード類に1回だけ暗号鍵データと出力帰還データの初期値とを設定する手段を設けたことを特徴とする請求項1記載のカード類の所有者確認方法。

【請求項3】 前記カード類に比べて前記携帯物の出力帰還データが余分に更新される場合のために、前記カード類の出力帰還データを更新しつつ前記携帯物から受信した出力帰還データと複数回比較することを特徴とする請求項1記載のカード類の所有者確認方法。

【請求項4】 前記カード類が前記携帯物に比べて出力帰還データが余分に更新されるのを防ぐために、カード類に暗号化機能とその逆の復号機能を合せ持つ手段を設け、該カード類で利用不可の判定が下った時、該カード類の出力帰還データを当該確認開始時の元の出力帰還データへ戻すことを特徴とする請求項3記載のカード類の所有者確認方法。

【請求項5】 前記カード類が前記携帯物に比べて出力帰還データが余分に更新されるのを防ぐために、カード類に当該確認開始時の出力帰還データを保持する手段を設け、該カード類で利用不可の判定が下った時、該カード類の出力帰還データを当該確認開始時の元の出力帰還データへ戻すことを特徴とする請求項3記載のカード類の所有者確認方法。

【請求項6】 前記カード類と前記携帯物との確認処理と、利用可となってからのカード類と情報処理装置との相互処理に一定時間の間隔を許容するため、前記カード

2

類に、該カード類を一定時間だけ利用可状態とし、該一定時間内に情報処理装置との相互処理が開始されないと自動的に利用不可状態にする手段を設けたことを特徴とする請求項1記載のカード類の所有者確認方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、カード類を利用する情報処理サービスシステムなどにおいて、特に、利用可と利用不可の状態をとり、利用可の場合に情報処理装置に対して処理を依頼でき、処理終了で利用不可となるカード類を使用する場合の所有者確認方法に関する。

【0002】

【従来の技術】 従来、情報処理サービスシステムにおける個人確認の代表例としては、情報処理サービス分野でのコンピュータ端末からセンターへアクセスする時のパスワードや、キャッシュカード利用時に於ける暗証番号による確認などが知られている。しかし、コンピュータ利用のパーソナル化の進展に伴い、人間の忘却性、複数利用時の煩雑性、他人によるパスワード推測可能性などが問題になってきている。

【0003】 これらの要求条件を満たす個人確認技術に必須な構成要素としては、ICカードを代表とするカード類が有効である。ここで、カード類とは、キャッシュカード、クレジットカード、プリペイドカードなど現在利用されている磁気タイプのカードや、データ入出力を抑制するインテリジェント機能を付加できるLSIを組み込んだICカードなどが挙げられる。

【0004】 限界ある個人の記憶情報に比べて、ICカードに組み込める暗証子のデータ量は膨大であるため、最近の暗号・暗証研究の成果であるRSA法、FS法など（例えば、辻井、佐原編著：“暗号と情報セキュリティ”、昭晃堂、1990、参照）によれば、高い確度で確認相手（対象装置）に対してカード類の識別を行うことが可能に成ってきている。

【0005】

【発明が解決しようとする課題】 ところで、情報処理装置等の対象装置に対してカード類を確認する機能が発達しても、真の所有者だけが利用できるようにならなければ安全ではない。従来のカード類の所有者確認方法は、図14に示すように、記憶情報（暗証番号等）、所有物（クレジットカード、免許証等）、身体的特徴（指紋、筆跡等）に分類され、記憶情報や所有物が多用されている。このうち、記憶情報は人間の記憶のあいまいさに起因する問題がある。又、身体的特徴も、指紋等身体的特徴を対象とするパターン認識の研究は盛んであるが、操作性、コスト、確実性の観点から現状では解決すべき課題が多い。これに対し、個人の所有物による方法は実現的な解であるが、カード類の所有者を明らかにするための有効な手段が存在しないのが現状である。

【0006】 本発明の目的は、カード類では実現できな

い身体的特徴に匹敵する携帯性と、人間の記憶以上の確実性とを備え、複製しにくく紛失に気付き易い携帯物によるカード類の所有者確認方法を提供することにある。

【0007】

【課題を解決するための手段】上記目的を達成するために、本発明は、カード類の状態が利用可と利用不可の2種類あり、利用可の場合に該カード類により情報処理装置に対して処理を依頼でき、処理終了で利用不可となるとして、カード類の所有者が携帯する携帯物に、あらかじめ定められた暗号鍵データを格納する手段と、あらかじめ定められた初期値をとり、その後更新される出力帰還データを格納する手段と、前記暗号鍵データにより前記出力帰還データを暗号化して更新する手段と、前記更新された出力帰還データを前記カード類に送信する手段とを設け、カード類には、前記携帯物が送信した出力帰還データを受信する手段と、あらかじめ定められた暗号鍵データを格納する手段と、あらかじめ定められた初期値をとり、その後更新される出力帰還データを格納する手段と、前記暗号鍵データにより前記出力帰還データを暗号化して更新する手段と、前記更新された出力帰還データと前記携帯物から受信した出力帰還データとを比較して、当該カード類の利用可または利用不可を決定する手段とを設け、前記携帯物とカード類の暗号鍵データ、出力帰還データの初期値を一致させ、所有者の処理要求の度に、前記携帯物の出力帰還データと前記カード類の出力帰還データを更新せしめて同期をとることを主たる特徴とするものである。

【0008】

【作用】本発明では、従来から用いられている個人識別のためのカード類に加えて、当該カード類の利用者であることを保証する手段として携帯物を導入し、携帯物とカード類で、あらかじめ同一の暗号鍵データと出力帰還データの初期値を共有し、該携帯物とカード類においてそれぞれ更新される出力帰還データを同期させることで、自動的に当該カード類の所有者確認を行う様にしたので、使用者の負担を増加させることなく、安全性の高い所有者確認を行うことが可能になる。

【0009】

【実施例】以下、本発明の実施例を図面にもとづいて詳細に説明する。図1は本発明の所有者確認方法を実施するシステムの基本構成の概念図を示したものである。図において、1はカード類所有者の携帯物、2は確認対象のカード類、3は目的の処理を実行する情報処理装置である。携帯物1としては、例えば、時計、ネクタイピン、指輪、またはブローチ等の装身具を用いて、これらの装身具内に処理/記憶手段を埋め込んで作る。また、カード類2としては、データ入出力等を任意に抑制するインテリジェント機能を付加できるICカードを挙げることが出来る。これらの携帯物1とカード類2との結合は、電氣的、光学的、または電磁的方法のいずれによっ

ても良い。

【0010】正当な使用権を有する個人がカード類2により情報処理装置3を利用しようとする場合、当該利用者は、自分の携帯物1を用いてカード類2に自らが正当な所有者であることを確認させ、該確認されたカード類（利用可状態のカード類）2を情報処理装置3に接続等して目的の処理を依頼する。カード類2と情報処理装置3は相互に確認しあつた後、情報処理装置3において目的の処理を実行し、それが完了すると、カード類2は利用不可状態となる。

【0011】図2に、所有者確認を行う場合の携帯物1とカード類2での処理概要を示す。同一所有者の携帯物1とカード類2には、あらかじめ同じ暗号鍵データと出力帰還データの初期値を記憶しておく。この携帯物1とカード類2の出力帰還データは、その後、所有者確認のたびに更新されるが、当該携帯物1とカード類2の処理が同期している限り、内容の一致性が保証される。

【0012】通常、カード類2は利用不可状態にある。該カード類2を用いて情報処理装置3に処理を依頼する場合、まず、利用者は携帯物1とカード類2を起動する。これは、利用者自身により携帯物1とカード類2の両方を起動してもよいし、図2に示すように、カード類2へは携帯物1から結合手段を介して確認要求を出すことでよい。起動を受けた携帯物1は、記憶されている暗号鍵データにより出力帰還データを暗号化して前の出力帰還データを更新すると共に、該更新された出力帰還データをカード類2に送信する。カード類2でも、記憶されている暗号鍵データにより出力帰還データを暗号化して前の出力帰還データを更新するが、この更新された出力帰還データと携帯物1から送られた出力帰還データ（確認情報）とを照合し、一致したなら当該カード類2を利用可状態にする。このようにして、正当な所有者であることが確認されたなら、利用者は当該カード類2を情報処理装置3に接続して目的の処理を依頼する。そして、情報処理装置3での処理が完了すると、カード類2は自から利用不可状態に戻る。

【0013】以下に、本発明の所有者確認方法を実施するための種々のシステム構成を示す。

【0014】図3は本発明の第1の実施例の構成図である。携帯物1は、制御部100、鍵レジスタ101、暗号化処理部102、送信部103、確認依頼受容部104、出力帰還データ（OFB）レジスタ110から構成される。カード類2は、制御部200、鍵レジスタ201、暗号化処理部202、受信部203、利用権情報管理部205、個人情報登録部206、情報処理装置対応処理部207、通信部208、OFBレジスタ210、照合部211から構成される。また、情報処理装置3は、制御部300、個人情報登録部301、カード類対応処理部302、通信部303、目的処理部304から構成される。携帯物1とカード類2との接続手段12

は、電気的、光学的、電磁的等のいずれによっても良い。

【0015】所有者確認を行う前の前提条件として、携帯物1の鍵レジスタ101とカード2の鍵レジスタ201には同一の暗号鍵を格納し、同様に、携帯物1のOFBレジスタ110とカード2のOFBレジスタ210には同一の出力帰還データの初期値を格納しておく。各出力帰還データは、暗号鍵により暗号化処理された結果で更新されるため、OFBレジスタ110、210の出力帰還データは変化したが、該各出力帰還データを初期値で一致させれば、その後、同期して暗号化処理される限り、携帯物1とカード2で一致が保証される。

【0016】カード2の所有者確認を行う場合、利用者は確認依頼受容部104を介して携帯物1へカード利用依頼を行い、カード2へは携帯物1から接続手段12を経由して確認要求を出力するか、利用者自らがカード2へ確認要求を行うかして、結果的に携帯物1ならびにカード2の制御部100、200が各処理部分を起動する。これにより、携帯物1では、暗号化処理部102がOFBレジスタ110に格納されている出力帰還データを鍵レジスタ101に格納されている暗号鍵データで暗号化して更新し、該更新された出力帰還データを再びOFBレジスタ110に格納する。同時に、該携帯物1の暗号化処理部102で更新された出力帰還データは、送信部103から送信され、接続手段12を介してカード2の受信部208で受信される。カード2では、同様に暗号化処理部202がOFBレジスタ210に格納されている出力帰還データを鍵レジスタ201に格納されている暗号鍵データを暗号化して更新し、該更新された出力帰還データを再びOFBレジスタ210に格納する。さらに、該カード2では、暗号化処理部202で更新された当該カード2の出力帰還データと受信部208で受信された携帯物1の出力帰還データとを照合部211で比較し、両者が一致する場合、利用権情報管理部205のカード利用状態を利用可状態へ切り替える。これでカード2の利用が可能になる。

【0017】カード2が正当な所有者により使用されていることが確認されて、利用者がカード2を情報処理装置3に接続すると、各制御部200、300の制御下で、以下の手順で処理が実行される。即ち、まず、カード2と情報処理装置3では、個人情報管理部206、301に管理されている個人情報をもとに、情報処理装置3の暗号化処理部207とカード2の暗号化処理部302で個人識別交換データを生成して、通信部208、303を介して交換し、相互に相手を確認しあう。そして、最終的に情報処理装置3のカード2暗号化処理部302がカード2を正当と確認すると、次に、目的処理部304が当該カード2の正当な所有者の求めている処理を実行し、それが完了すると、通信部303を介してカード2に対して処理完了を通知する。カード2の情報処

理装置3の暗号化処理部207は、情報処理装置3より通信部208を介して処理完了を受け取ると、利用権情報管理部205のカード利用状態を利用不可状態へ戻す。

【0018】図4は、上述の処理フローをカード2について表したものである。なお、図中で「携帯物出力情報不適合を表示」とあるのは、カード2が情報処理装置3において目的処理を実行できなかったことで結果的に示すか、カード2に接続される情報処理装置3経由で利用者に表示することなどを指す。

【0019】図3の実施例は、 $x \leftarrow ek(x)$ (x を暗号鍵 K で暗号化して更新することを示す)で更新される出力帰還データは、例えば第三者がある時の出力帰還データを知っても、暗号鍵 K を知らない限り、次の出力を推定することは困難であるという考えに基づいている。しかし、 x の数列が短い周期の循環になる場合等、暗号化処理部102、202が実行する暗号化関数によっては、その関数に内在するアルゴリズム構造の欠陥を利用して、第三者が携帯物1からカード2への送信データを推定する可能性は完全に排除できない。このような場合には、接続手段12として電気接点による接続か、非接触の場合でも、指向性の高い電磁波(光波、赤外線等を含む)、超音波を用いる。この場合、携帯物1を所持する所有者が、携帯物の送信データを意図的に第三者に観測させない限り、観測が究めて困難となる。

【0020】図5は本発明の第2の実施例の構成図で、図3の構成においてカード2内に1タイム書き込み部204を付加したものである。

(1)安全上、カード2と携帯物1とは異なる者が発行した方が一元的に秘密情報が管理される心配が無く好ましい。

(2)運用上等の要請で、カード2と携帯物1との使用期間が異なる場合がある。

などの理由により、携帯物1とカード2が、同時に発行されない場合がある。

【0021】図5に於いては、その様な場合でも、カード2に1タイム書き込み部204を備えることにより、携帯物1とカード2との出力帰還データ同士の間隔をとることが可能になる。即ち、カード2に於て、携帯物1が保持している鍵レジスタ101に格納される暗号鍵とOFBレジスタ110に格納される出力帰還データを、1タイム書き込み部204により最初の一回に限りそれぞれ鍵レジスタ201とOFBレジスタ210に設定できるようにする。具体的には、書き込みが終了すると、ヒューズROMにデータが書込まれるか、内部の論理処理を司る書き込みルーチンを消去させるなどで、外部からカード2の鍵レジスタ201、OFBレジスタ210に対して書き込みができない状態として、1回だけの書き込みを可能とする。なお、携帯物1内のOFBレジスタ110が可成り更新された後に、新規のカード2と対応付ける必要がある時、この1回だけの書

き込み時に限り、カード類2のOFBレジスタ210の更新を多く繰り返すことで対応させる。

【0022】図6は本発明の第3の実施例の構成図で、図3の構成においてカード類2内にカウンタ処理部209を付加したものである。

(1) 複数のカード類2に携帯物1を対応付けたい。

(2) 不用意な操作で携帯物1の出力隣接データが更新される可能性がある。

などの理由により、携帯物1とカード類2に格納される出力隣接データが同期しない場合がある。このような場合、一般に携帯物1の出力隣接データが余計に更新される。

【0023】図6においては、カード類2にカウンタ処理部209を備えることにより、携帯物1の出力隣接データが余計に更新されていても、カード類2での出力隣接データの更新を所定回数繰り返すことで、正当な所有者を確認できる。

【0024】図7に、カウンタ処理部209を付加した場合のカード類2における処理フローを示す。カード類2では、携帯物1が出力する出力隣接データと一致照合されるまで、該カード類内部で出力隣接データを更新する。適合しない携帯物を確認する場合、実用での携帯物における更新回数の上限をしきい値THとして設定し、そのしきい値までカード類の出力隣接データを更新しつつ一致照合をおこない、全て不一致なら適合しない携帯物と判定する。

【0025】図8は本発明の第4の実施例の構成図で、図6の構成において、カード類2の暗号化処理部202を暗号化/復号処理部202'に置き換えたものである。

【0026】図6の実施例では、対応付けられていない携帯物との照合によりカード類2の出力隣接データが更新されるが、この対策としては携帯物1の出力隣接データを更新すればよいことが考えられる。しかし、携帯物1の更新に、多大な操作または時間を要する場合など、携帯物更新が困難である場合、携帯物1よりカード類2の出力隣接データが余分に更新されることが、本所有者確認のシステムを構築する上での障害となることがある。このような場合、図8のように、カード類2の暗号化処理部を暗号化/復号処理部202'とすることにより、対応付けられていない携帯物と照合された時に生じるカード類2の出力隣接データの著しい更新を補償することができる。

【0027】図9に、カウンタ処理部209に加え、暗号化処理部を暗号化/復号処理部202'に置き換えた場合のカード類2における処理フローを示す。カード類2に於いて、毎回行われる所有者確認では、携帯物1が出力する出力隣接データと一致照合されるまで、該カード類内部で出力隣接データを更新し、適合しない携帯物と判定された場合、カウンタの値が示す回数だけ、前回

正規の携帯物と確認した状態まで出力隣接データを、復号処理により返す。

【0028】図10は本発明の第5の実施例の構成図で、図6の構成において、カード類2内にOFBレジスタ210の他にサブOFBレジスタ210'を追加したことである。本実施例の狙いは、図8の第4の実施例と同様に、カード類内の出力隣接データの更新が進み過ぎない様にする手段を提供することにある。図11に、図10の場合のカード類2における処理フローを示す。カード類2に於いて、毎回行われる所有者確認では、携帯物1が出力する出力隣接データと一致照合されるまで、該カード類内部で出力隣接データを更新し、適合しない携帯物が判定された場合、前回の利用可と判定された携帯物確認時の出力隣接データを格納していたサブOFBレジスタ210'の値を読み出し、OFBレジスタ210に格納されていた値を元の出力隣接データへ戻す。なお、適合する携帯物と判定された場合は、サブOFBレジスタ210'に、更新された出力隣接データが収容されたOFBレジスタ210の値を書き込み、両者の値を一致させる。

【0029】図12は本発明の第6の実施例の構成図で、図3の構成においてカード類2内のタイマー212を付加したものである。

【0030】携帯物1とカード類2間の所問者確認と、カード類2と情報処理装置3間の個人識別とは同時に行う必要がなく、両者の処理を行う場所が物理的に離れている方が好ましい場合がある。この為、図12の実施例に於いては、所有者確認をしてから個人識別処理を行うまでの適当な期間を測定できるタイマー212をカード類2内に備えるようにしたものである。

【0031】図13に、タイマー212に関係するカード類2内の処理フローを示す。カード類2に於いて、カード類利用可状態へ切り替わった後で、タイマー212が0にリセットされ、最大許容経過時間以下の時間経過内に、目的処理の始まりである個人確認処理に移れば、正規の利用ができる。逆に最大許容経過時間より時間が経過すると、カード類は利用不可状態へ切り替わる。

【0032】

【発明の効果】(1) 請求項1の発明によれば、カード類では実現できない身体的特徴に匹敵する携帯性と、人間の記憶以上の確実性を備えた記憶手段として、時計、ネクタイピン、ブローチ等の装身具を携帯物を用いて、それに所定の機能を組み込み、対応するカード類と同期をとることで、当該カード類の所有者確認を行うようにしたので、使用者の負担を増加させることなく、安全性の高い所有者確認を行うことができる。また、印鑑と同様の感覚で携帯物を利用できるため、指紋、顔形等の身体的特徴に比べ、人々に受け入れられ易い利点がある。さらに、装身具の形により多様な形態が可能であり応用範囲が広い利点もある。

9

【0033】(2) 請求項2の発明によれば、携帯物とカード類が同時に発行されない場合においても、携帯物とカード類との出力側データ同士の間隔をとることができる。

【0034】(3) 請求項3の発明によれば、一つの携帯物を複数のカード類に対応付けした場合や、不意な操作で携帯物の出力側データが更新された場合などにより、携帯物とカード類の出力側データが同期していない場合でも、支障なく所有者確認チェックを行うことができる。

【0035】(4) 請求項4および5の発明によれば、請求項3において、対応付けられていない携帯物との照合によりカード類の出力側データが余分に更新される場合、自動的に確認チェック開始時の元の出力側データへ戻すことができる。

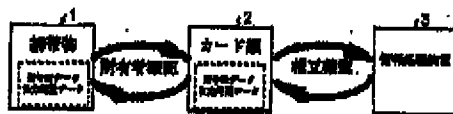
【0036】(5) 請求項6の発明によれば、カード類と携帯物との確認処理と、利用可となったからのカード類と対象装置との相互処理に一定時間の間隔を許容するため、両者の処理を行う場所を物理的に離すことができる。

【図面の簡単な説明】

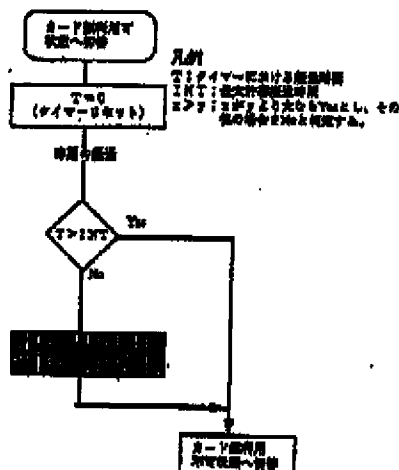
【図1】本発明が実施されるシステムの基本構成図である。

【図2】図1における携帯物とカード類の処理概要を示す図である。

【図1】



【図13】



10

【図3】本発明の第1の実施例の具体的構成図である。

【図4】図3におけるカード類の処理フロー図である。

【図5】本発明の第2の実施例の具体的構成図である。

【図6】本発明の第3の実施例の具体的構成図である。

【図7】図5におけるカード類の処理フロー図である。

【図8】本発明の第4の実施例の具体的構成図である。

【図9】図8におけるカード類の処理フロー図である。

【図10】本発明の第5の実施例の具体的構成図である。

【図11】図10におけるカード類の処理フロー図である。

【図12】本発明の第6の実施例の具体的構成図である。

【図13】図12におけるカード類内のタイマに関係する処理フロー図である。

【図14】従来のカード類の所有者確認方法の一例を示した図である。

【符号の説明】

1 携帯物

2 カード類

3 情報処理装置

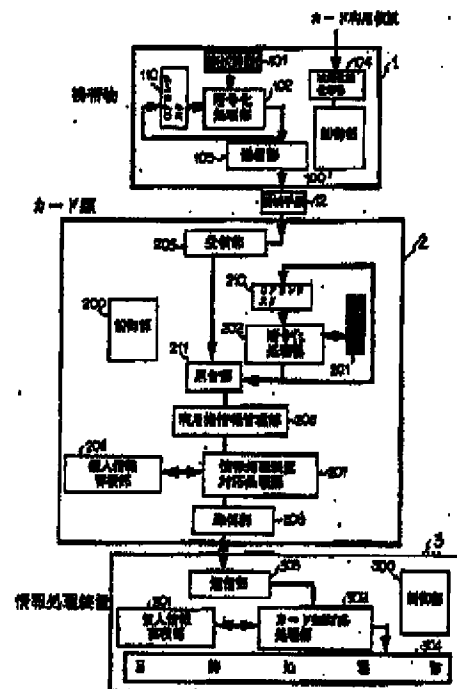
101, 201 鍵レジスタ

102, 202 暗号化処理部

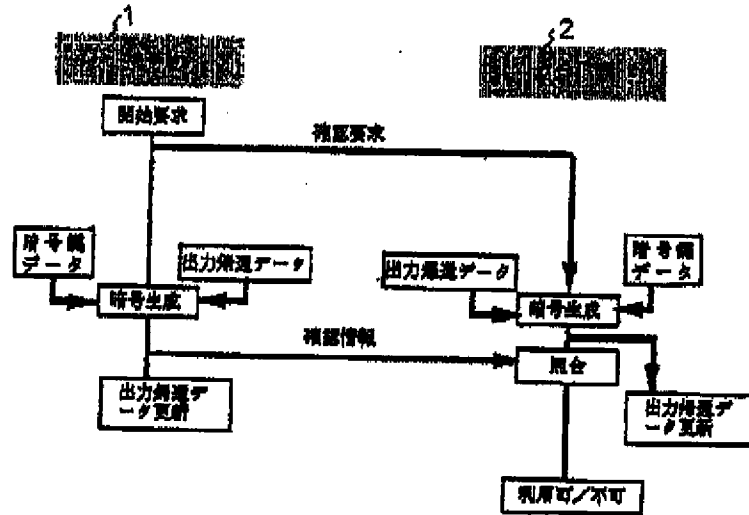
210 出力側データ (OFB) レジスタ

111 照合部

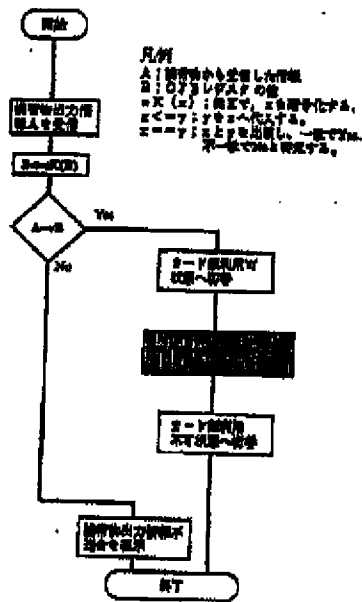
【図3】



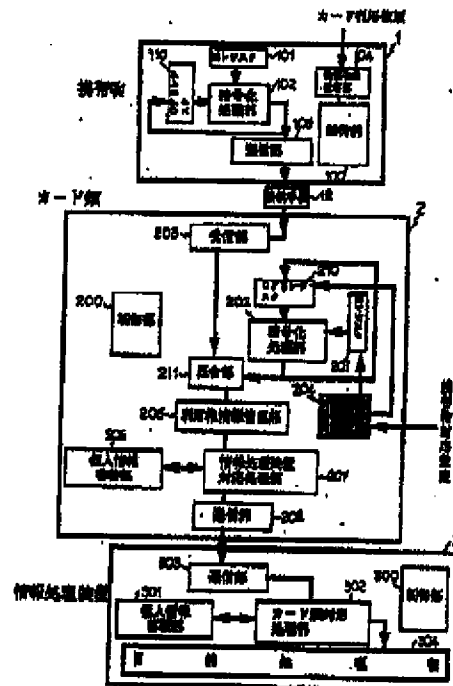
【図2】



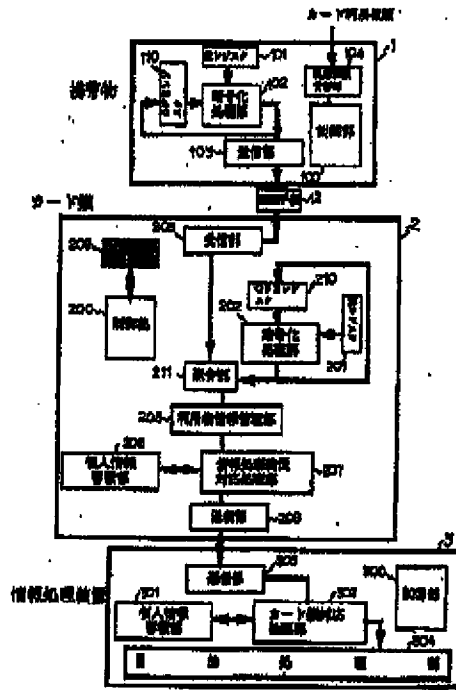
【図4】



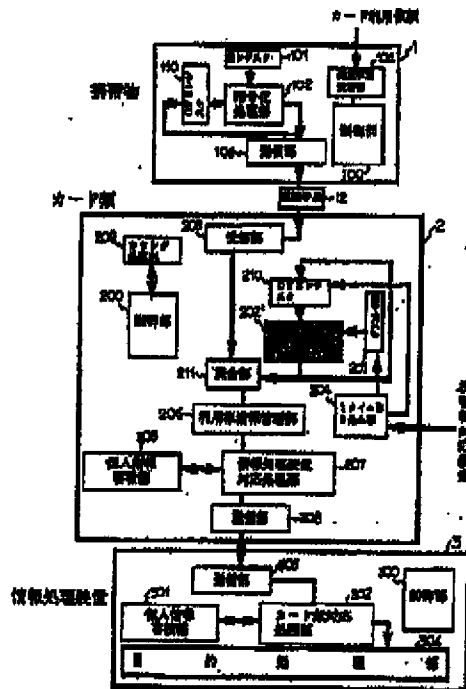
【図5】



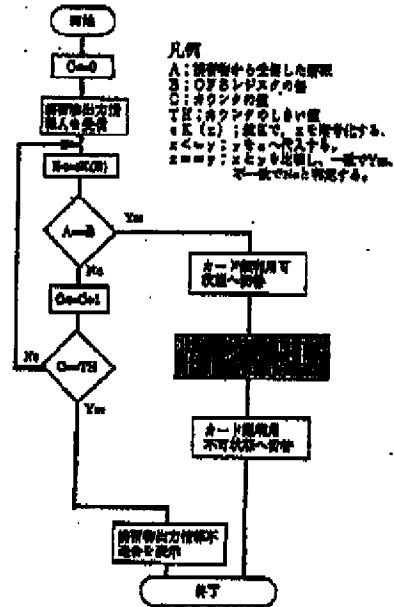
【図6】



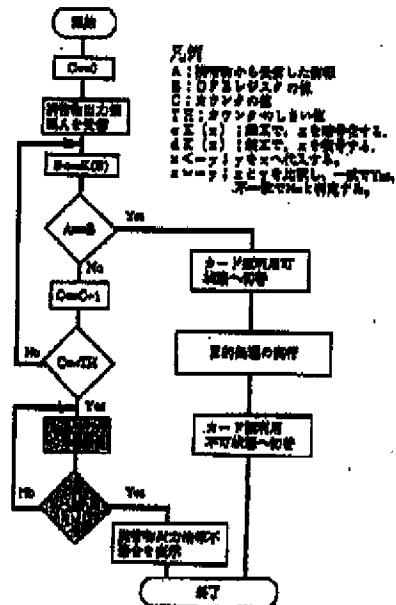
【図7】



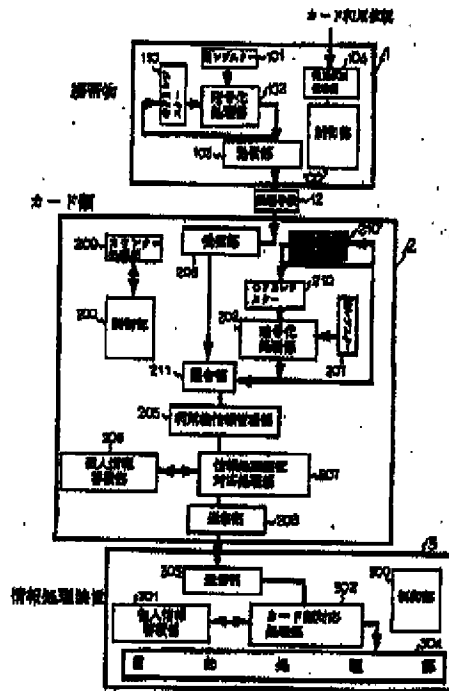
【図7】



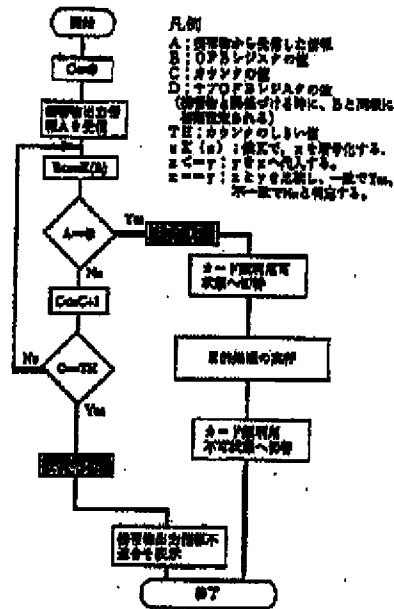
【図9】



【圖 10】

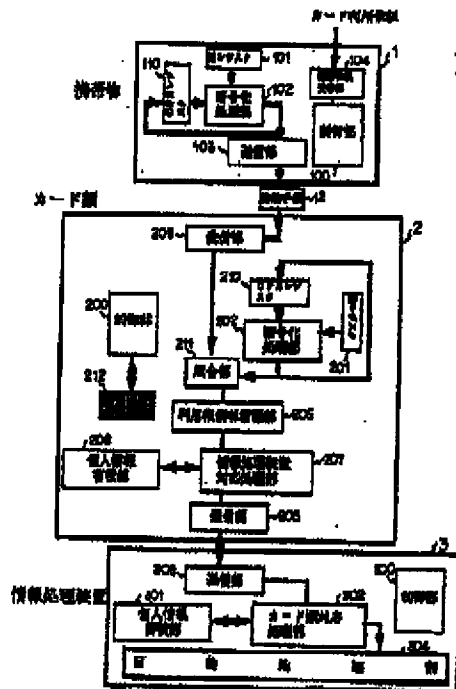


[REDACTED]



【图 14】

【圖 12】



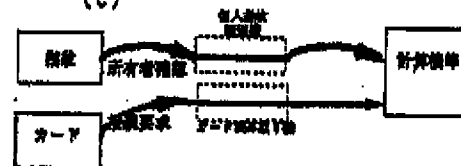
(2)



(b)



(c)



フロントページの続き

(5) Int. Cl.⁵

G 0 6 K 17/00

G 0 7 F 7/12

G 0 9 C 1/00

識別記号

片内接連番号

F I

技術表示箇所

S 8823-5L

7922-5L